

**THE UNITED STATES DISTRICT COURT FOR THE  
WESTERN DISTRICT OF MISSOURI**

**IN THE MATTER OF THE  
SEARCH OF: E-MAIL ACCOUNT  
"DEPUTYJONES33@GMAIL.COM"  
MAINTAINED BY GOOGLE INC.**

**AFFIDAVIT IN SUPPORT OF SEARCH WARRANT**

I, Charles Root, a Task Force Officer (TFO) with the Federal Bureau of Investigation (FBI),  
being duly sworn, hereby depose and state as follows:

1. I have been employed as a police officer with the City of Joplin, Missouri, since 2004 and a sworn law enforcement officer since 1994. I am currently a Task Force Officer (TFO) with the Federal Bureau of Investigation (FBI) as well as the Southwest Missouri Cyber Crimes Task Force in Joplin, Missouri. I have been assigned to investigate computer crimes, including violations against children. I have gained expertise conducting such investigations through training in seminars, classes, and everyday work related to these types of investigations. I have attended training provided by the FBI Cyber Crime Division, the FBI's Regional Computer Forensic Laboratory, and the Missouri Internet Crimes Against Children (ICAC) Task Force. I have written, executed, and assisted in over 200 search warrants on the state and federal level.
2. As a TFO, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.
3. The statements in this affidavit are based on my personal observations, my training and experience, my investigation of this matter, and information obtained from other agents

and witnesses. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth the facts that I believe necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2251, 2252(a) and 2252A(a) are located in user account "deputyjones33@gmail.com."

4. I am investigating activities occurring on Google Inc. (hereinafter "Google"), e-mail address "deputyjones33@gmail.com." There is probable cause to believe the registrant of the aforementioned account has produced, received, possessed, and/or transmitted child pornography, in violation of 18 U.S.C. §§ 2251, 2252, and 2252A. Affiant submits this affidavit in support of a search warrant authorizing a search of the Google e-mail account "deputyjones33@gmail.com," which is described below and in Attachment A, for the items specified in Attachment B hereto, which items constitute contraband, instrumentalities, fruits, and evidence of the foregoing violations. Affiant is requesting authority to search the entire Google e-mail account "deputyjones33@gmail.com," where the items specified in Attachment B may be found, and to seize all items listed in Attachment B as contraband, instrumentalities, fruits, and evidence of crime.
5. I have probable cause to believe that evidence of violations of 18 U.S.C. §§ 2251, 2252, and 2252A, involving the use of a computer in or affecting interstate commerce to produce, receive, possess, and/or transmit child pornography, is located in and within the aforementioned property described below. Thus, as outlined below, and based on my training and experience, there is probable cause to believe that evidence, fruits and/or

instrumentalities of the aforementioned crimes are located in this property.

### **STATUTORY AUTHORITY**

6. This investigation concerns alleged violations of Title 18, U.S.C., §§ 2251, 2252, and 2252A, relating to material involving the sexual exploitation of minors:
  - a. 18 U.S.C. § 2251(a) prohibits a person from employing, using, persuading, inducing, enticing or coercing a minor to engage in sexually explicit conduct for the purpose of producing any visual depiction of such conduct, if such person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce, or if such visual depiction actually was transported in or affecting interstate commerce.
  - b. 18 U.S.C. § 2252 prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any visual depiction of minors engaging in sexually explicit conduct when such visual depiction was either mailed or shipped or transported in interstate or foreign commerce by any means, including by computer, or when such visual depiction was produced using materials that had traveled in interstate or foreign commerce.
  - c. 18 U.S.C. § 2252A prohibits a person from knowingly mailing, transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any child pornography, as defined in 18 U.S.C. §2256(8), when such child pornography was either mailed or shipped or transported in interstate or

foreign commerce by any means, including by computer, or when such child pornography was produced using materials that had traveled in interstate or foreign commerce.

### **DEFINITIONS**

7. The following definitions apply to this Affidavit and its Attachments:
- a. The term "minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.
  - b. The term "sexually explicit conduct," 18 U.S.C. § 2256(2)(A)(i-v), is defined as actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person.
  - c. The term "visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.
  - d. The term "computer," as defined in 18 U.S.C. §1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related

to or operating in conjunction with such device.

- e. The term "child pornography," as defined in 18 U.S.C. § 2256(8), means any visual depiction, including any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where

1. the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;
2. such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or
3. such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

- f. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing), or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks,

CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

- g. "Internet Service Providers" (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.
- h. "Internet Protocol address" (IP address), as used herein, is a code made up of numbers separated by dots that identifies a particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.
- i. "Domain names" are common, easy to remember names associated with an IP address. For example, a domain name of "www.usdoj.gov" refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period.
- j. "Website" consists of textual pages of information and associated graphic

images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

### **BACKGROUND ON GOOGLE INC. GMAIL SERVICES**

8. Google is a commercial computer service company headquartered in 1600 Amphitheatre Parkway, Mountain View, California, which provides services including e-mail and Groups to Internet users.
9. In my training and experience, I have learned that Google provides a variety of on-line services, including electronic mail ("e-mail") access, to the general public. Google's e-mail service is labeled Gmail. Gmail allows subscribers to obtain e-mail accounts at the domain name "gmail.com," like the e-mail account listed in Attachment A. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and un-retrieved e-mail for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, e-mail transaction information, and account application information. Once registered, a user obtains a unique Google identification (ID) (sometimes referred to as a screen name, login name, or profile). Several profiles can be associated with a single Google ID. The profiles are also known as aliases and allow the user to appear as someone other than their Google, Inc. ID when using certain Google services. Other users of the service may be able to view profile information. A Google users' registration and profile information are

supplied by the user and is not verified by Google.

10. Users of Gmail may also access other Google services through their account such as, Google Drive, Google Docs, Picassa, You Tube, and Google Photo, Within these services, users may join chat rooms and groups that allow them to chat (through Google Hangouts) via video, audio, or instant messaging with other Google users.

### **BACKGROUND OF THE INVESTIGATION**

11. On September 25, 2015, Southwest Missouri Cyber Crimes Task Force Officer (TFO) Brian Martin opened an investigation on CyberTip 6329521. The CyberTip was originally filed with the National Center for Missing and Exploited Children (NCMEC), the national clearinghouse for such reports, by Dropbox, Inc. (hereinafter "Dropbox") on August 21, 2015.
12. TFO Martin reviewed the CyberTip from NCMEC. According to the CyberTip, Dropbox had discovered many video and image files that they believed contained child pornography. The files were discovered in an account with the username "Juan Jines," with an account ID of 196266196. The e-mail associated with the account is man\_cardinal@yahoo.com. The account was established on July 25, 2013, and it is a free account. Dropbox reported two IP addresses were used to upload the video and image files; IP address 172.56.10.225 was used on December 15, 2014, and IP address 172.56.12.46 was used on April 26, 2015. Both of these IP addresses are registered to T-Mobile. An Investigative Subpoena was sent to T-Mobile to determine the holder of the IP address. T-Mobile advised their IP addresses are not user specific, merely gateways to the Internet.



13. TFO Martin reviewed the thirteen files submitted by Dropbox with the Cybertip. All of the files contained what he believed to be child pornography. A brief description of three files is provided below:

- a. File one is entitled "Buena Fiesta.3gp" and is a video file. The video shows a prepubescent female and a prepubescent male sitting on a couch or bed. There are adult voices heard in the background. Shortly into the film, the two children begin engaging in vaginal and anal intercourse.
- b. File two is entitled "fernanda h 07 by spooky - by tlz(2).avi" and is a video file. The video shows a prepubescent female on a webcam. removing her clothes and simulating sexual intercourse. Her breasts, vagina, and anus are displayed. The child appears to be engaging in a chat session with someone who is telling her what to do.
- c. The third file is entitled "ptxx) 2014\_02\_tlz\_hpim0003.avi" and is a video file. The video shows a prepubescent female lying on her back with her vagina exposed. She tries to open what appears to be a bottle of baby oil and has to have someone help her open it. After getting the bottle open, she pours some oil on her vagina and puts some on a vibrator. She is also seen putting her fingers inside her vagina.

14. On January 6, 2016, members of the SMCCTF served a federal search warrant for 2685 East Atlantic Street, Springfield, Missouri. While the warrant was being executed, TFO Chip Root and TFO Martin made contact with Juan Jones (hereinafter "Jones") at his place of employment, the Greene County Sheriff's Office. TFO Root and TFO Martin

met with Jones in an interview room. After being advised of the search warrant, and his *Miranda* rights, Jones agreed to speak with TFO Root and TFO Martin. Jones admitted that he had looked at child pornography for as long as ten years. He identified his e-mail address as man\_cardinal@yahoo.com. He admitted to having a Dropbox and Tumblr account, and he admitted that he had stored child pornography within those accounts. Jones stated he had met individuals on the file sharing site Tumblr with whom he exchanged child pornography images.

15. He stated he used his cellular phone, a Samsung SM-N900T, when he looked at the child pornography. Jones admitted he used a Verizon hot spot for Internet connection. During the forensic examination of the phone, which utilized an Android mobile operating system, the forensic examiner determined Jones utilized an e-mail address of "deputyjones33@gmail.com." The forensic examiner was able to locate titles of files associated with various Google services that were utilized by "deputyjones33@gmail.com." Some of the titles observed by the examiner included common child pornography search terms in the titles such as, "13yo masturbates" and "4yo pussy drink."

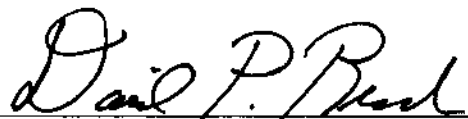
**PROBABLE CAUSE**

16. Based on the above facts, I believe probable cause exists for the issuance of a warrant to search the premises described more fully in Attachment A for (1) property that constitutes evidence of the commission of a criminal offense; (2) contraband, the fruits of a crime, or things otherwise criminally possessed; and/or (3) property designated or intended for use or which is or has been used as the means of committing a criminal offense, namely possible violations of 18 U.S.C. §§ 2251, 2252, and 2252A, including but not limited to the items listed in Attachment B.



Charles Root  
Task Force Officer  
Federal Bureau of Investigation

Subscribed and sworn before me this 22<sup>nd</sup> day of ~~January~~<sup>February</sup>, 2016.



Honorable David P. Rush  
United States Magistrate Judge  
Western District of Missouri

***ATTACHMENT A***  
***PROPERTY TO BE SEARCHED***

The e-mail account "deputyjones33@gmail.com" maintained by Google Inc.,  
headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043.

**ATTACHMENT B**  
**LIST OF ITEMS TO BE SEIZED AND SEARCHED**

**I. Information to be disclosed by Google Inc.:**

To the extent that the information described is within the possession, custody, or control of Google Inc., Google Inc. is required to disclose the following information to the government for the e-mail account: deputyjones33@gmail.com:

- a. The contents of all text messages, voice-mail, e-mails and instant messages stored in the account, including copies of communications and text messages sent to and from the account, drafts, the source and destination addresses associated with each e-mail or text message, the date and time at which each e-mail or text message was sent, and the size and length of each e-mail or text message, and any images, photographs, jpg files, gif files, tif files, avi files, and mpeg files video files;
- b. All records or other information regarding the identification of the Google account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

- c. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and
- d. All records pertaining to communications between Google, Inc., and any person regarding the account, including contacts with support services and records of actions taken.

**II. Information to be seized by Government Agents:**

All information described above in Section I that consists of fruits, evidence and, instrumentalities of violations of 18 U.S.C. §§ 2251 and 2252, including the following:

- a. Information pertaining to the production, possession, transportation, receipt, advertisement, or viewing of visual depictions involving the use of a minor engaging in sexually explicit conduct; and
- b. Records relating to the identities and locations of any persons who created, used, or communicated using the account.

**III. Method of Service**

- a. Google Inc. shall disclose responsive data, if any, by sending to data to an address designated by case agent FBI TFO Charles Root using the US Postal Service or another courier service, notwithstanding 18 U.S.C. 2252A or similar statute or code.